Arithmétique dans un anneau de polynômes

Thierry Veyt
Math Partage*

Louvain-la-Neuve, 20 février 2017

La méthode des idempotents

En utilisant la méthode des idempotents, on démontre le théorème d'existence des polynômes d'interpolation simple.

Théorème La fonction polynômiale passant par les points $(x_i,\ y_i)$ est définie comme suit :
$P(x) = \Sigma_{i=1}^{n} y_i \Pi_{j,j\neq i} \frac{X - x_j}{x_i - x_j}$

démonstration La division polynômiale peut s'écrire de la manière suivante :
$P = D.Q + R$ avec $P, D, Q, R \in A[X]$
On peut utiliser comme diviseur le monôme $(x - x_i)$:
$P(x) = (x - x_i) . Q + R$ Les points $(x_{i,\ y_i})$ appartenant à la fonction polynômiale, ils vérifient cette fonction, c'est-à-dire que l'on peut effectuer la valuation de cette fonction en x_i:
$P(x_i) = (x_i - x_i) . Q + R$. Or $P(x_i) = y_i = R$
On peut donc écrire l'équation comme suit:
$P(x) = (x - x_i) . Q + y_i$. y_i est donc le reste de la division du polynôme par $(x - x_i)$. Cela permet l'écriture modulaire suivante :
$P(x) = y_i \ mod \ (x - x_i)$
L'existence d'idempotents assurée par le théorème des restes chinois, avec les conditions de co-maximalité, nous permet d'écrire :
$\begin{cases} e_i = 0 + Q . (X - x_j) \ \forall j \neq i.(1) \\ e_i = 1 + Q . (X - x_i) \end{cases}$ $\begin{cases} e_i = 0 \ mod \ (X - x_j) \ \forall j \neq i \\ e_i = 1 \ mod \ (X - x_i) \end{cases}$

*Math Partage est un réseau d'entraide et d'échange de documents mathématiques entre étudiants et anciens étudiants de l'université de Franche-Comté

En valuant chaque polynôme $e_i(x)$ par la valeur x_i, nous pouvons calculer la valeur de Q :
$e_i(x_i) = 1 + Q \cdot (x_i - x_i) = 1$. Mais aussi :
$e_i(x_i) = 0 + Q \cdot (x_i - x_j)$. En combinant ces deux valeurs nous obtenons :
$Q = \frac{1}{(x_i - x_j)}$. Et donc en remplaçant dans (1)
$e_i(x) = \frac{(X - x_j)}{(x_i - x_j)}$ Etant donné la structure modulaire des solutions, c'est-à-dire
$\begin{cases} P_i(x) = 0 \; mod \; (X - x_j) \; \forall j \neq i \\ P_i(x) = y_i \; mod \; (X - x_i) \end{cases}$ $P_i(x) = y_i \begin{cases} e_i(x) = 0 \; mod \; (X - x_j) \; \forall j \neq i \\ e_i(x) = 1 \; mod \; (X - x_i) \end{cases}$
Nous concluons que $P(x) = \Sigma_{i=1}^{n} P_i(x) = \Sigma_{i=1}^{n} y_i . \; e_i(x)$. Et donc nous arrivons à la formulation du théorème ci-dessus.

Equation de la droite passant par 2 points par la méthode de Lagrange

$\begin{cases} e_1 \cong 0 \; mod \; (x - x_1) \\ e_1 \cong 1 \; mod \; (x - x_2) \end{cases}$ $\begin{cases} e_2 \cong 1 \; mod \; (x - x_1) \\ e_2 \cong 0 \; mod \; (x - x_2) \end{cases}$
$e_1 = \lambda \; (x - x_1) = 1 + \lambda'(x - x_2)$ Valuons le polynôme $e_1(x)$ par sa valeur en x_2 dans les deux expressions
$e_1(x_2) = \lambda(x_2 - x_1) = 1$
De là on tire la valeur de lambda : $- > \lambda = \frac{1}{x_2 - x_1}$
$e_1(x) = \frac{x - x_1}{x_2 - x_1}$
$e_2 = \mu \; (x - x_2) = 1 + \mu'(x - x_1)$
Valuons le polynôme $e_2(x)$ par sa valeur en x_1 dans les deux expressions.
$e_2(x_1) = \mu(x_1 - x_2) = 1$
De là on tire la valeur de mu :
$- > \mu = \frac{1}{x_1 - x_2}$
$e_2(x) = \frac{x - x_2}{x_1 - x_2}$
De là, on trouve la valeur de y(x) :
$y(x) = y_1 \frac{x - x_2}{x_1 - x_2} + y_2 \frac{x - x_1}{x_2 - x_1}$

Equation d'une parabole passant par 3 points par la méthode de Lagrange

Exercice résolu

Soient les points (1,3) , (-1,2) , et (2,-1). Calculer l'une des deux paraboles qui passent par ces trois points en calculant d'abord les multiplicateurs de Lagrange qui sont des polynômes orthogonaux de degré minimum. Vérifier qu'ils sont bien orthogonaux dans l'anneau-quotient $\frac{\mathbb{Z}[X]}{(X-1)(X+1)(X-2)}$ et que leur somme est bien égale à 1. Vérifier également que ces polynômes sont bien idempotents dans ce même anneau-quotient. Montrer que l'isomorphisme entre $\frac{\mathbb{Z}[X]}{(X-x_i)} \times \frac{\mathbb{Z}[X]}{(X-x_j)} \times ...$ et $\frac{\mathbb{Z}[X]}{(X-x_i)(X-x_j)...}$ (avec $i \neq j$) aboutit bien à la construction de polynômes idempotents

Résolution

Recherche des multiplicateurs de Lagrange.

$\begin{cases} e_1(x) = 1 \ mod \ (X - x_1) \\ e_1(x) = 0 \ mod \ (X - x_2)(X - x_3) \end{cases}$ $\begin{cases} e_1(x) = 1 \ mod \ (X - 1) \\ e_1(x) = 0 \ mod \ (X + 1)(X - 2) \end{cases}$

Valuons $e_1(x)$ en x_1

$\begin{cases} e_1(x_1) = 1 + Q.\,(x_1 - x_1) = 1 \\ e_1(x_1) = 0 + Q.\,(x_1 - x_2)(x_1 - x_3) \end{cases}$ $\begin{cases} e_1(x_1) = 1 \\ e_1(x_1) = Q.\,(1 + 1)(1 - 2) \end{cases}$

Nous obtenons $Q = \frac{-1}{2}$

Nous obtenons en remplaçant Q[1] dans l'équation modulaire $e_1(x) = \frac{-1}{2}\,(X + 1)(X - 2)$ c'est-à-dire

$e_1(x) = \frac{-1}{2}\,x^2 + \frac{1}{2}\,x + 1$

$\begin{cases} e_2(x) = 1 \ mod \ (X - x_2) \\ e_2(x) = 0 \ mod \ (X - x_1)(X - x_3) \end{cases}$ $\begin{cases} e_2(x) = 1 \ mod \ (X + 1) \\ e_2(x) = 0 \ mod \ (X - 1)(X - 2) \end{cases}$

Valuons $e_2(x)$ en x_2

$\begin{cases} e_2(x_2) = 1 + Q'.\,(x_2 - x_2) = 1 \\ e_2(x_2) = 0 + Q'.\,(x_2 - x_1)(x_2 - x_3) \end{cases}$ $\begin{cases} e_2(x_2) = 1 \\ e_2(x_2) = Q'.\,(-1 - 1)(-1 - 2) \end{cases}$

Nous obtenons $Q' = \frac{1}{6}$

Nous obtenons en remplaçant Q'[2] dans l'équation modulaire $e_2(x) = \frac{1}{6}\,(X - 1)(X - 2)$ càd

$e_2(x) = \frac{1}{6}\,x^2 + \frac{-1}{2}\,x + \frac{1}{3}$

$\begin{cases} e_3(x) = 1 \ mod \ (X - x_3) \\ e_3(x) = 0 \ mod \ (X - x_1)(X - x_2) \end{cases}$ $\begin{cases} e_3(x) = 1 \ mod \ (X - 2) \\ e_3(x) = 0 \ mod \ (X - 1)(X + 1) \end{cases}$

[1] $e_1(x) = 0 \ mod \ (X + 1)(X - 2)$ c'est-à-dire $e_1(x) = Q.\,(X + 1)(X - 2)$
[2] $e_2(x) = 0 \ mod \ (X - 1)(X - 2)$ càd $e_2(x) = Q'.\,(X - 1)(X - 2)$

Valuons $e_3(x)$ en x_3

$\begin{cases} e_3(x_3) = 1 + Q''.\ (x_3 - x_3) = 1 \\ e_3(x_3) = 0 + Q''.\ (x_3 - x_1)(x_3 - x_2) \end{cases}$ $\begin{cases} e_3(x_3) = 1 \\ e_3(x_3) = Q''.\ (2 - 1)(2 + 1) \end{cases}$

Nous obtenons $Q'' = \frac{1}{3}$

Nous obtenons en remplaçant Q[3] dans l'équation modulaire $e_3(x) = \frac{1}{6}\ (X - 1)(X - 2)$ c'est-à-dire

$e_3(x) = \frac{1}{3}\ x^2 - \frac{1}{3}$

La fonction polynômiale est donc $P(x) = y_1.e_1(x) + y_2.e_2(x) + y_3.e_3(x)$

C'est-à-dire :

$P(x) = 3.(\frac{-1}{2}\ x^2 + \frac{1}{2}\ x + 1) + 2.(\frac{1}{6}\ x^2 + \frac{-1}{2}\ x + \frac{1}{3}) - 1.(\frac{1}{3}\ x^2 - \frac{1}{3})$

Nous obtenons $P(x) = \frac{-3}{2}\ x^2 + \frac{1}{2}\ x + 4$ Les points (1,3) , (-1,2) , et (2,-1) appartiennent bien à la parabole recherché[4].

Vérifions que les multiplicateurs de Lagrange sont bien orthogonaux dans $\frac{\mathbb{Z}[X]}{(X+1)(X-1)(X+2)}$

Sachant que $e_1(x) = Q.\ (X + 1)(X - 2)$, que $e_2(x) = Q'.\ (X - 1)(X - 2)$, et que $e_3(x) = Q''.\ (X - 1)(X + 1)$, nous prouvons aisément que :

$e_1(x).e_2(x) = Q.Q'\ (X + 1)(X - 2)^2(X - 1) = S.\ (X + 1)(X - 2)(X - 1) = 0\ mod\ (X + 1)(X - 2)(X - 1)$

On montre la propriété de projectivité en sommant les $e_i(x)$:

$\Sigma_{i=1}^{3} e_i(x) = (\frac{-1}{2}\ x^2 + \frac{1}{2}\ x + 1) + (\frac{1}{6}\ x^2 + \frac{-1}{2}\ x + \frac{1}{3}) + (\frac{1}{3}\ x^2 - \frac{1}{3})$

$\Sigma_{i=1}^{3} e_i(x) = (\frac{-1}{2} + \frac{1}{6} + \frac{1}{3})\ x^2 + (\frac{1}{2} - \frac{1}{2})\ x + 1 = 1$

On vérifie l'idempotence des $e_i(x)$ en montrant que $e_i^2(x) = e_i(x)\ mod(X-1)(X+1)(X-2)$

Après élévation au carré et division euclidienne par (X-1)(X+1)(X-2), on obtient bien que :

$e_1^2(x) = (\frac{-1}{2}\ x^2 + \frac{1}{2}\ x + 1)^2 = \frac{1}{4}\ x^4 - \frac{1}{2}\ x^3 - \frac{3}{4}\ x^2 + x + 1$

$e_1^2(x) = (\frac{-1}{2}\ x^2 + \frac{1}{2}\ x + 1) + \frac{1}{4}\ x\ (x^3 - 2x^2 - x + 2)$

$e_1^2(x) = (\frac{-1}{2}\ x^2 + \frac{1}{2}\ x + 1) + Q.(X-1)(X+1)(X-2)$

$e_1^2(x) = (\frac{-1}{2}\ x^2 + \frac{1}{2}\ x + 1)\ mod\ (X-1)(X+1)(X-2)$

On vérifie également que :

$e_2^2(x) = \frac{1}{36}\ x^4 - \frac{1}{6}\ x^3 + \frac{13}{36}\ x^2 - \frac{1}{3}\ x + \frac{1}{9}$

$e_2^2(x) = \frac{1}{6}\ x^2 + \frac{-1}{2}\ x + \frac{1}{3} + (\frac{1}{36}\ x - \frac{1}{9})(x^3 - 2x^2 - x + 2)$

$e_2^2(x) = e_2(x)\ mod\ (X-1)(X+1)(X-2)$

De même :

$e_3^2(x) = \frac{1}{9}\ x^4 - \frac{2}{9}\ x^2 + \frac{1}{9}$

$e_3^2(x) = \frac{1}{3}\ x^2 - \frac{1}{3} + (\frac{1}{9}\ x + \frac{2}{9})(X-1)(X+1)(X-2)$

[3] $e_3(x) = 0\ mod\ (X - 1)(X + 1)$ càd $e_3(x) = Q''.\ (X - 1)(X + 1)$

[4] Le lecteur le vérifiera aisément en valuant le polynôme

$e_3^2(x) \;=\; e_3(x) \; mod \; (X-1)(X+1)(X-2)$

Pour montrer l'idempotence dans le cas général, on utilise les définitions de $e_i(x)$:

$\begin{cases} e_i(x) \cong 1 \; mod \; (X-x_i) \\ e_i(x) \cong 0 \; mod \; (X-x_j)(X-x_k)...avec \; i \neq j,k,... \end{cases}$

$e_i^2(x) = [1 \; mod \; (X-x_i)][0 \; mod \; (X-x_j)(X-x_k)...]$

$e_i^2(x) = [1 + Q.(X-x_i)][Q'.(X-x_j)(X-x_j)...]$

$e_i^2(x) = Q'.(X-x_j)(X-x_j)... + Q.Q'(X-x_i)(X-x_j)(X-x_k)...$

$e_i^2(x) = e_i(x) \; mod \; (X-x_i)(X-x_j)(X-x_k)...$

Exercice et plan de résolution

Calculer l'équation de l'autre parabole passant par ces trois points.

Résolution

La parabole sera de type $x = ay^2 + by + c$. On peut utiliser la formule de Lagrange, en tenant compte que "x" joue le rôle de "y" et que "y" joue le rôle de "x" càd : $P(y) \;=\; \Sigma_{i=1}^n x_i \Pi_{j,j\neq i} \frac{Y \;-\; y_j}{y_i \;-\; y_j}$. Ou calculer (plus long) l'équation modulaire qui sera de type :

$\begin{cases} e_1(y) \;=\; 1 \; mod \; (Y \;-\; y_1) \\ e_1(y) \;=\; 0 \; mod \; (Y \;-\; y_2)(Y \;-\; y_3) \end{cases}$ $\begin{cases} e_2(y) \;=\; 1 \; mod \; (Y \;-\; y_2) \\ e_2(y) \;=\; 0 \; mod \; (Y \;-\; y_1)(Y \;-\; y_3) \end{cases}$

$\begin{cases} e_3(y) \;=\; 1 \; mod \; (Y \;-\; y_3) \\ e_3(y) \;=\; 0 \; mod \; (Y \;-\; y_1)(Y \;-\; y_2) \end{cases}$

Pour obtenir une équation de type y = f(x), il faut inverser la fonction. On procède de la sorte :

On écrit d'abord le polynôme sous forme unitaire c'est-à-dire $x = y^2 + \frac{b}{a}y + \frac{c}{a}$. Ensuite, on cherche à l'exprimer sous la forme $(y \;+\; \alpha)^2$ + terme indépendant.

$x = (y^2 + \frac{2b}{2a}y + \frac{b^2}{4a^2}) - \frac{b^2}{4a^2} + \frac{c}{a}$

$x = (y + \frac{b}{2a})^2 - (\frac{b^2-4ac}{4a^2})$

$(y + \frac{b}{2a})^2 \;=\; x \;+\; (\frac{b^2-4ac}{4a^2})$

$(y + \frac{b}{2a}) \;= \pm\sqrt{x \;+\; (\frac{b^2-4ac}{4a^2})}$

$y \;=\; -\frac{b}{2a} \;\pm\; \sqrt{x \;+\; (\frac{b^2-4ac}{4a^2})}$

References

[1] Gras, Georges et Marie-Nicole, *Arithmétique, Algèbre fondamentale*, 2004, Ellipses.

[2] Kostrikin, A., *Introduction à l'algèbre*, 1981,Editions de Moscou, traduit en français du russe par V.Kolimeev

[3] Godement, Roger, *Cours d'algèbre*, 1966, Hermann

e-mail : thierryveyt@gmail.com